

FILED**UNITED STATES DISTRICT COURT****JUN 1 2018**for the
Northern District of Oklahoma**Mark C. McCartt, Clerk
U.S. DISTRICT COURT**

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*THE PREMISES LOCATED AT 1616 EAST YOUNG
STREET, APARTMENT 123, TULSA, OKLAHOMA

Case No.

*18-mj-74-PJC***APPLICATION FOR A SEARCH WARRANT**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment "A":

located in the _____ Northern _____ District of _____ Oklahoma _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment "B":

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

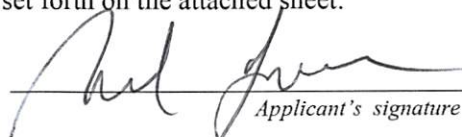
The search is related to a violation of:

| <i>Code Section</i> | <i>Offense Description</i> |
|---------------------------|--|
| 18 U.S.C. § 2252(a)(2) | Distribution and/or Receipt of Child Pornography |
| 18 U.S.C. § 2252(a)(4)(B) | Possession of Child Pornography |

The application is based on these facts:
See Affidavit of Michael Lelecas, Special Agent, United States Department of Homeland Security (DHS),
Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI)

☒ Continued on the attached sheet.

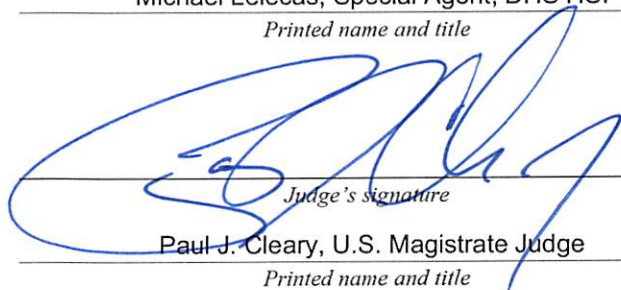
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

*Applicant's signature*

Michael Lelecas, Special Agent, DHS HSI

Printed name and title

Sworn to before me and signed in my presence.

Date: 06/01/2018City and state: Tulsa, Oklahoma*Judge's signature*

Paul J. Cleary, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Michael Lelecas, a Special Agent (SA) with Homeland Security Investigations (HSI), being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a special agent with the United States Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI). Prior to this appointment, I was a Special Agent or Inspector with the Immigration and Naturalization Service (INS) from April 1996 until September 2000. I am currently assigned to the Resident Agent in Charge (RAC), Tulsa, Oklahoma. Within this office, I conduct investigations in numerous areas of federal law to include, but not limited to, narcotics, immigration, financial fraud, child exploitation, and gangs. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) including those on computer media. Moreover, I am a federal law enforcement officer who enforces criminal laws, including 18 U.S.C. § 2252A and am authorized by the Attorney General to request a search warrant.

2. During my tenure as a criminal investigator, your affiant has participated as a case agent and support agent in numerous investigations covering various areas of criminal law. During these investigations, your affiant has participated in interviewing witnesses and cooperating sources regarding these various crimes, and your affiant has read official reports of similar

interviews by other officers. Your affiant has participated in surveillance operations, observing and recording movements of persons involved in criminal activity. Your affiant has authored search warrants, seizure warrants, and other court orders in furtherance of criminal investigations your affiant has participated in. Additionally, your affiant has spoken to other agents who have experience with child pornography cases. Your affiant has learned that people who obtain child pornography often save and maintain those images on their electronic devices for substantial periods of time. Moreover, your affiant is a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252 and 2252A.

3. This affidavit is submitted in support of an application for a search warrant for the locations specifically described in Attachment A of this Affidavit, including the entire properties located at **1616 East Young Street apartment 123, Tulsa, Oklahoma** (herein after the “SUBJECT PREMISES”) for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1) (distribution and/or receipt of a visual depiction of a minor engaged in sexually explicit conduct) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), which items are more specifically described in Attachment B of this Affidavit.

4. The statements in this affidavit are based in part on information provided by the Toronto Police Service (TPS), HSI Toronto and my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, your affiant has not included each and every fact known to me concerning this investigation. Your affiant has set forth only the facts that your affiant believes are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations 18 U.S.C. §§ 2252(a)(2) and (b)(1) (distribution and/or receipt of a visual depiction of a minor engaged in sexually explicit

conduct) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), are presently located at the SUBJECT PREMISES.

**BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS,
THE INTERNET, AND EMAIL**

5. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras and smartphones with cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store in excess of 300 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the

camera or on a removable memory card. The video files can be easily transferred from the camcorder to a computer.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP's) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (*i.e.*, "instant messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files

on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or “burn” files onto them). Media storage devices can easily be concealed and carried on an individual’s person. Smartphones and/or mobile phones are also often carried on an individual’s person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user’s computer or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an e-mail as a file on the computer or saving the location of one’s favorite websites in, for example, “bookmarked” files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user’s Internet activities generally leave traces or “footprints” in the web cache

and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

h. A device known as a router in conjunction with a modem allows numerous computers to connect the Internet and other computers through the use of telephone, cable, or wireless connection. A router, in conjunction with a modem, can connect literally millions of computers around the world. Routers often store information as to which computer used a modem to connect to the Internet at a specific time and location. This information when viewed along with the traces or “footprints” can provide valuable information on who distributed and/or received a visual depiction of a minor engaged in sexually explicit conduct and who possessed and accessed with intent to view a visual depiction of a minor engaged in sexually explicit conduct.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

6. Based upon my training and experience, and information relayed to me by agents and others involved in the forensic examination of computers, your affiant knows that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to “cloud” storage. Your affiant also knows that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and

make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

7. Based on your affiant’s experience and your affiant’s consultation with other agents who have been involved in computer searches, searching computerized information for contraband, evidence, fruits, or instrumentalities of a crime often requires the seizure of all of a computer system’s input and output peripheral devices, related software, documentation, and data security devices (including passwords), so that a qualified computer expert can accurately retrieve the system’s data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware

drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). Further, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

8. Additionally, based upon your affiant's training and experience and information relayed to me by agents and others involved in the forensic examination of computers, your affiant knows that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, your affiant knows that individuals who have set up either a secured or

unsecured wireless network in their residence are often among the primary users of that wireless network.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

9. In April 2017, HSI Tulsa received information from HSI Toronto regarding Kik user “rickmuddemon”. Kik is a messaging application that allows users to send messages one on one or in a group setting. Users can send text, images, or videos via the application. The Toronto Police Service (TPS) served a search warrant on or after October 2016 on a Canadian Citizen, Benjamin Faulkner, who was the administrator of a Tor board that was involved in distributing child abuse material (CAM) on a Tor board. A Tor board is a website on the “dark web” that can’t be accessed without a special browser and knowledge of the board’s Tor address. Common internet search engines such as Google are not able to search information contained on the Tor network.

10. Pursuant to the search warrant of Faulkner’s residence numerous electronic devices were seized and searched by TPS. As a result of the TPS examination of these devices, 25 files were located, which had filenames created by the Kik messenger application. TPS served a production order to Kik to obtain the original poster’s information, to include: IP addresses and email addresses utilized on Kik by the individuals.

11. As a result of the production order served on Kik, TPS learned that on April 29, 2015, rickmuddemon uploaded one file to a Kik group that was located within a device seized from Faulkner. The file posted by rickmuddemon was a video depicting a child, that TPS believed to be approximately 4 years old, laying her back with no underwear and her vagina

exposed. An adult male is standing over the child masturbating in view of the female child. SA Lelecas has viewed this video as well and also concluded that it depicts sexual abuse of a child.

12. Pursuant to the same production order described above, Kik provided that rickmuddemon utilized email addresses doghandler@yahoo.com, dread68@aol.com, Rickbeyard@aol.com, and rickbeyard@yahoo.com while utilizing the Kik application. Kik also provided the last IP address captured while rickmuddemon was utilizing Kik to be 174.255.132.219 on March 16, 2017.

13. TPS conducted open source research on Facebook. TPD entered rickbeyard@yahoo.com into the search bar of Facebook and located a profile for Rick Beyard, who is utilizing this email address and appeared to be residing in Tulsa, Oklahoma.

14. HSI Tulsa SA Perez conducted a query of the Oklahoma driver's license database for Rick Beyard and located an Oklahoma identification card issued to Beyard under number U994189553. Beyard provided the SUBJECT PREMISES as his address on his identification card. SA Lelecas obtained a copy of the photo associated to Beyard's identification card. Photos of Beyard on the profile match the photo of Beyard on his Oklahoma issued identification card.

15. On November 07, 2017, DHS Summons ICE-HSI-TV-2018-00007 was served to Verizon wireless requesting, in part, all information pertaining to IP address 174.255.132.219 on March 16, 2017. Verizon doesn't issue IP addresses to each individual cellular telephone that accesses the internet, rather Verizon assigns the IP address based on the user's location. As a result, numerous devices can be associated to one IP address at any given time. Verizon provided compliance to HSI in the form of an Excel spreadsheet listing every telephone number that connected to IP address 174.255.132.219 on March 16, 2017.

16. On May 16, 2018, SA Perez interviewed an employee at the Town Square Apartment office which serves as the leasing office for the SUBJECT PREMISES. The employee confirmed that Beyard lives at the SUBJECT PREMISES and has been a resident for more than a year. The employee stated that Beyard lives with his daughter and home schools her. The employee provided Beyard's telephone number, 918-894-2100. Beyard provided this telephone number on his leasing application.

17. A review of the above described Excel spreadsheet provided by Verizon revealed 918-894-2100 as being associated to IP address 174.255.132.219 on March 16, 2017. This is the same IP address and date when rickmuddemon connected to Kik.

18. Beyard is also found to have existing city traffic related warrants, listing that he resides at the SUBJECT PREMISES.

19. On May 16, 2018, SA's Perez and Lelecas went to the SUBJECT PREMISES and walked by the SUBJECT PREMISES to obtain a physical description of the residence. While walking by the apartment, SA Perez saw an individual, who matched the description of Beyard standing in the doorway of the SUBJECT PREMISES.

20. Based upon the email address utilized for the Kik profile "rickmuddemon" being the same as the Facebook profile for Beyard, your affiant believes that Beyard is the user of rickmuddemon and distributed the above described video to a Kik group. Your affiant further asserts that Beyard is residing at the SUBJECT PREMISES. Your affiant knows through his training and experience in child exploitation investigations that individuals such as Beyard will maintain their collection of child exploitation material for extended periods of time. Even though it has been more than three years since Beyard was last observed distributing child

exploitation material, your affiant asserts that Beyard's continued use of the associated Kik account indicates that a search of the SUBJECT PREMISES will likely result in the discovery of evidence that will aid in the prosecution of Beyard.

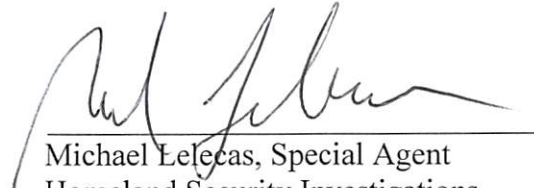
CONCLUSION

21. Based upon the above-described facts and circumstances, Your affiant believes that a search warrant served upon the SUBJECT PREMISES will aid law enforcement in identifying the devices utilized by Beyard to chat on Kik in furtherance of this crime. Your affiant knows from his experience in chat based investigations, such as this one, that data can often be recovered from a device once it is deleted. Your affiant believes that a search of the SUBJECT PREMISES will likely result in the discovery of the devices utilized by Beyard and will likely result in the discovery of child exploitation material. Your affiant further believes that a forensic exam of these devices will likely result in the discovery of evidence.

22. Therefore, your affiant asserts there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

23. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain

a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.



Michael Lelecas, Special Agent
Homeland Security Investigations

Sworn and subscribed before me this 1st day of June, 2018.



PAUL J. CLEARY
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT "A"

The residence to be searched is **1616 East Young Street apartment 123, Tulsa, Oklahoma 74106**. The residence is the lower unit in a two-story apartment complex. The number "1616" is affixed to the northeast wall of the apartment building. The target apartment is on the first floor on the southwest side of the building. The number "123" is affixed to the front door of the apartment which faces southwest. The back door of the apartment is on the south side of the building.

The premises to be searched includes any appurtenances to the real property that is the **SUBJECT PREMISES of 1616 East Young Street apartment 123, Tulsa, Oklahoma 74106**, and any storage units/outbuildings or vehicles associated with the **SUBJECT PREMISES**.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

- A. Images of child pornography or child erotica; files containing images; and data of any type relating to the sexual exploitation of minors, and material related to the possession thereof, in any form wherever it may be stored or found including, but not limited to:
- i. Any cellular telephone, smartphone, tablet, personal digital assistant, computer, computer system and related peripherals; computer hardware; computer software; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, printers, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems, hard drives and other computer related operation equipment, digital cameras, scanners, external storage devices, routers, modems, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums; any input/output peripheral devices, including but not limited to computer passwords and data security devices and computer-related documentation, and any hardware/software manuals related to or used to: visually depict child pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography, or information pertaining to an interest in child pornography;
 - ii. Books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors;
 - iii. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors; and
 - iv. Stories, text-based files, motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors;
- B. Information, correspondence, records, documents or other materials pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to the sexual exploitation of minors, that were transmitted or received using computer, cellular device, personal

digital assistant, or some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

- i. Envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors; and
- ii. Books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors;
- iii. Any and all records, documents, or materials, including any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce including by United States mail or by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256 or relating to the sexual exploitation of minors;
- iv. Any and all records, documents, or materials, including any and all address books, names, and lists of names and addresses of minors visually depicted while engaging in sexually explicit conduct, defined in Title 18, United States Code, Section 2256; or relating to the sexual exploitation of minors;
- v. Any and all records of Internet usage including user names and e-mail addresses and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage mediums, including CDs or DVDs;
- vi. Any physical keys, encryption devices, dongles and similar physical items necessary to access computer equipment, storage devices or data;
- vii. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data; and
- viii. Files, records, programs, logs, electronic communications, scanning programs, financial records, hacking software, or router configuration software;

- C. Credit card information including but not limited to bills and payment records, including but not limited to records of internet access;
- D. Records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence;
- E. Records or other items which evidence ownership or use of computer equipment or any of the devices described in this attachment that are found in the above residence, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes;
- F. Any and all adapters, chargers or other hardware items necessary to charge the battery, or to maintain the functioning of, any of the equipment described above; and
- G. Any data or materials establishing ownership, use or control of any computer equipment seized from **1616 East Young Street apartment 123, Tulsa, Oklahoma 74106.**
- H. Any and all information, correspondence (including emails), records, documents and /or other materials related to contacts, in whatever form, with minors involving the production, possession and /or distribution of child pornography and the attempt or act of educating, enticing, coercing, or persuading a minor to engage in sexual acts.
- I. Any article of clothing or other item observed in the video sent by the user "rickmuddemon".